Solutions to odd-numbered exercises
Peter J. Cameron, *Introduction to Algebra*, Chapter 1

1.1 This exercise should really have been marked with two stars! Apologies for starting the book with such a hard exercise.

We begin with a lemma.

Lemma *Any point is on at least three lines.*

Proof We are given that there are three non-collinear points; let us call them A, B, C. We show first that each of these points lies on at least three lines.

The lines AB, AC and BC are all distinct. Now BC doesn't pass through A, so there is a unique line through A parallel to BC. Thus, A lies on at least three lines. The same applies to B and C.

Now let P be any point; we show that P lies on at least three lines. There is a line joining P to A. If this line is AB, then P, A, C are not collinear, so each lies on at least three lines. Similarly if this line is AC. So we can assume that each of the lines joining P to A, B, C contains only one of these three points; so these three lines are all distinct. □

(a) To prove the statement, we argue by contradiction. First, if A is the statement 'every line passes through at least two points', then not-A is the statement 'some line passes through at most one point'. So we have two jobs to do. First, assume that L is a line passing through no points, and derive a contradiction; then assume that L is a line passing through just one point, and derive a contradiction.

Suppose that L passes through no points. Then the point A does not lie on L; so A lies on a unique line parallel to L. But since L contains no points, every line is parallel to it; so A lies on only one line, contradicting our lemma.

Now suppose that L passes through just one point P. We may suppose that $P \neq A$. Then A lies on a unique line parallel to L, and a unique line containing P; hence only two lines altogether, contradicting our Lemma.

(b) Take a line L. Choose any point P on L, and let L' be another line containing P. Then L and L' are not parallel. So every line parallel to L' must fail to be parallel to L (by Theorem 1.3), so that the number of points on L is equal to the number of lines parallel to L'.

Next, we show that if two lines L and L' are not parallel, then they contain the same number of lines. For L and L' meet at a point P, and by our strengthened lemma, there is a third line L'' containing P. Now the number of points on L is equal to the number of lines parallel to L''; but so is the number of points on L'. So these numbers are equal.

1.3 First we show that, if n is even, then n^2 is even. For suppose that n is even; say $n = 2m$. Then

$$n^2 = 4m^2 = 2(2m^2),$$

which is even since it is twice something (namely, twice $2m^2$).

Now for the converse: if n^2 is even then n is even. We replace this statement by its contrapositive (which is logically equivalent): if n is odd, then n^2 is odd. So let n be odd; say $n = 2m+1$. Then

$$n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1,$$

which is odd, as required.

1.5 (a) Just as in Pythagoras' proof, but we need a better version of the fact about odd and even numbers:

If n^2 is divisible by the prime number p, then n is divisible by p.

There is a more general form of this, which we will discuss in Chapter 2. You may assume it for now.

If the prime number p divides a product ab, then it divides either a or b.

Now if p divides $n^2 = n \cdot n$, then either p divides n or p divides n; that is, more simply, p divides n.

(b) Follow Pythagoras again. This time we need

If n^3 is even, then n is even.

This is for you!

1.7 Look ahead for the proof.

1.9 The argument is not valid. We have assumed the converse of Pythagoras' Theorem, i.e. if the sides a, b, c of a triangle satisfy $c^2 = a^2 + b^2$, then the triangle is right-angled.

We could make the argument valid by proving the converse of Pythagoras' Theorem; but that is another matter!

1.11 The computation is complicated but elementary. We have $(a+b\mathrm{i})^2 = (a^2 - b^2) + 2ab\mathrm{i}$. With $a = \sqrt{\frac{1}{2}(x + \sqrt{x^2+y^2})}$ and $b = \sqrt{\frac{1}{2}(-x + \sqrt{x^2+y^2})}$, we have

$$a^2 - b^2 = \frac{1}{2}(x + \sqrt{x^2+y^2}) - \frac{1}{2}(-x + \sqrt{x^2+y^2}) = x,$$

and

$$2ab = \sqrt{\left(x + \sqrt{x^2+y^2}\right)\left(-x + \sqrt{x^2+y^2}\right)} = \sqrt{-x^2 + x^2 + y^2} = y,$$

using the rule for the difference of two squares in the second line.

Of course, if x and y are real numbers, then $x^2 + y^2 \geq 0$, so $\sqrt{x^2+y^2}$ is a real number. Also, $x^2 \leq x^2 + y^2$, so $|x| \leq \sqrt{x^2+y^2}$; thus both $x + \sqrt{x^2+y^2}$ and $-x + \sqrt{x^2+y^2}$ are non-negative, so their square roots are real numbers also.

1.13(a) For $n = 0$, the sum of no numbers is 0, and $0 \times 1/2 = 0$, so the induction starts.

Suppose that the sum of the first n numbers is $n(n+1)/2$. Then the sum of the first $n+1$ numbers is

$$\frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2},$$

which is what we get by substituting $n+1$ for n in the formula.

(b) I don't know how to prove this directly by induction. Instead, use part (a); we have to show that

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}.$$

As usual, the induction starts.

Suppose that the equation above is true. Then

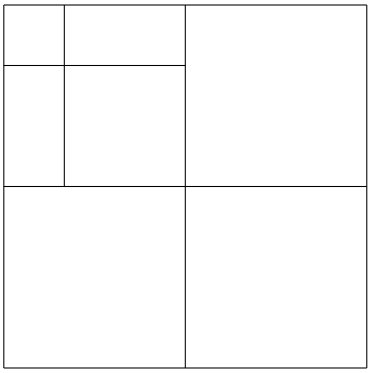
$$1^3 + \cdots + n^3 + (n+1)^3 = \frac{n^2(n+1)^2}{4} + (n+1)^3 = \frac{(n+1)^2(n+2)^2}{4},$$

after some manipulation.

Remark There is a geometric proof of this identity. If you take 1 square of side 1, 2 squares of side 2, ..., n squares of side n, then (after cutting one of the squares of each even side into two pieces) they can be fitted together to form a square of side $1+2+\cdots+n$. Thus

$$1 \cdot 1^2 + 2 \cdot 2^2 + \cdots + n \cdot n^2 = (1+2+\cdots+n)^2,$$

as required. Can you find how to do this? You can write it as an induction proof, since once you have done it for the squares with side up to n, you put the squares with side $n+1$ as a border along two sides of the big square. Here is the picture for $n = 3$:



1.15 (a) For $n = 1$, the left-hand expression is $1/3$, and so is the right-hand expression.

Suppose that the equation holds for the value n; that is, suppose that

$$\frac{1}{1 \times 3} + \frac{1}{3 \times 5} + \cdots + \frac{1}{(2n-1) \times (2n+1)} = \frac{n}{2n+1}.$$

Then

$$\begin{aligned}\frac{1}{1\times 3}+\cdots+\frac{1}{(2n+1)\times(2n+3)} &= \frac{n}{2n+1}+\frac{1}{(2n+1)(2n+3)}\\ &= \frac{n(2n+3)+1}{(2n+1)(2n+3)}\\ &= \frac{(n+1)(2n+1)}{(2n+1)(2n+3)}\\ &= \frac{n+1}{2n+3},\end{aligned}$$

[On the left, we have the sum of $n+1$ terms, of which the first n form the sum whose value we know by assumption. So the total is this sum plus the $n+1$st term.] The final expression is what is obtained by substituting $n+1$ for n in the expression on the right. So we have done the inductive step.

(b) For $n=4$, the two sides of the inequality are both equal to 256, so it is true. [Note that it is not true for $n=1,2,3$.]

For the inductive step, we see that in going from n to $n+1$, the left-hand expression is multiplied by 4. If we can show that the right-hand expression is multiplied by a factor which is not more than 4, we will get the required result. So we have to prove that $(n+1)^2/n^2 \le 4$. The proof goes like this: If $n \ge 4$, then

$$(n+1)^2 = n^2+2n+1 \le n^2+2n^2+n^2 = 4n^2,$$

since $2n \le 2n^2$ and $1 \le n^2$.

So, assuming the result for n, we have $4^n \ge 16n^2$, and so

$$\begin{aligned}4^{n+1} &= 4\cdot 4^n\\ &\ge 4\cdot 16n^2 \text{ by the induction hypothesis}\\ &= 16\cdot 4n^2\\ &\ge 16(n+1)^2 \text{ by what we just proved,}\end{aligned}$$

o the inductive step is done.

(c) For $n=2$, the left-hand expression is $1/(2^2-1)=1/3$, while the right-hand expression is $3/4-1/4-1/6=1/3$.

Suppose the result is true for n, that is,

$$\frac{1}{2^2-1}+\frac{1}{3^2-1}+\cdots+\frac{1}{n^2-1}=\frac{3}{4}-\frac{1}{2n}-\frac{1}{2(n+1)}.$$

Adding $1/((n+1)^2-1)$ to both sides gives

$$\frac{3}{4}-\frac{1}{2n}-\frac{1}{2(n+1)}+\frac{1}{n(n+2)}=\frac{3}{4}-\frac{1}{2(n+1)}-\frac{1}{2(n+2)},$$

since $1/(2n)-1/(n(n+2))=1/2(n+2)$.

1.17 The sequence of primes starting at $p_1 = 2$ is

$$2, 3, 7, 43, 13, 53, 5, 6221671$$

because

$2+1=3$ is prime;
$2\cdot 3+1=7$ is prime;
$2\cdot 3\cdot 7+1=43$ is prime;
$2\cdot 3\cdot 7\cdot 43+1=1807=13\cdot 139$;
$2\cdot 3\cdot 7\cdot 43\cdot 13+1=23479=53\cdot 443$;
$2\cdot 3\cdot 7\cdot 43\cdot 13\cdot 53+1=1244335=5\cdot 248867$;
$2\cdot 3\cdot 7\cdot 43\cdot 13\cdot 53\cdot 5+1=6221671$ is prime.

Proposition *Whatever prime we start with, we always obtain* 2 *in the sequence.*

Proof If we start with 2 (as above), then we certainly get it! Any other starting prime p would be odd; then $p+1$ is even, and its smallest prime factor is 2, so we would get 2 at the second stage. □

The question about whether 3 always arises is much harder, and there is no known proof that it always occurs.

We can say something. If we start with 3, of course we get it. If we start with 2, we get 3 at the second step.

Any other prime is of the form $6k+1$ or $6k+5$. [Why?] If we start with an odd prime of the form $6k+1$, we get 2 at the next step (as explained). Then at the following step, we take the smallest prime dividing $(6k+1)\times 2+1=12k+3$, which is obviously 3. But if we start with a prime of the form $6k+5$, at the next step we take the smallest prime dividing $12k+11$, which cannot be 3. You can continue this process for any number of steps without getting a guarantee that the prime 3 occurs.

For $p_1 = 5$, it takes four steps to arrive at 3: the primes we get are 5, 2, 11, 3. For $p_1 = 59$, it takes five steps; for $p_1 = 479$, it takes six; for $p_1 = 821$, it takes seven; for $p_1 = 1871$, it takes eight; but the numbers are too big for the computer to find a prime for which it takes nine steps to reach 3. The problem is that the intermediate numbers get very large!

This is the main difficulty in the calculation. For example, with $p_1 = 269$, we obtain the sequence

$$269, 2, 7, 3767, 3, 42559567, 1811316700667923$$

of primes, and the next value of N is 3280868190118528357557620466007, which is too big for the computer to factorise easily.

1.19 The argument is (obviously) not valid: I can clearly find two horses with different colours, so the inductive step from 1 to 2 must fail. Look at that step. For $n = 2$, we have $n-1=1$, so the purported argument says

- H_1 has the same colour (as itself), and
- H_2 has the same colour (as itself).

We can't conclude that H_1 and H_2 have the same colour. The argument given implicitly assumes that the sets $\{H_1,\ldots,H_{n-1}\}$ and $\{H_2,\ldots,H_n\}$ overlap; but for $n=2$ they don't.

1.21 Take $a=1$, $b=c=\frac{2}{3}$. Then

$$\begin{aligned} a\lfloor b+c\rfloor &= 1\times\lfloor\tfrac{4}{3}\rfloor &&= 1,\\ ab+ac &= \tfrac{2}{3}+\tfrac{2}{3} &&= \frac{4}{3},\\ \lfloor ab\rfloor+\lfloor ac\rfloor &= 0+0 &&= 0. \end{aligned}$$

1.23 In the previous exercise you have deduced the Remainder Theorem, so I will use that. If $f(x)=x^k-1$, then $f(1)=0$, so $x-1$ divides x^k-1 (as polynomials), which means that

$$x^k-1=(x-1)g(x)$$

for some polynomial $g(x)$ with integer coefficients. (Can you write down the polynomial $g(x)$?)

Substituting the natural number m for x, we find that $m^k-1=(m-1)g(m)$, and $g(m)$ is an integer; so $m-1$ divides m^k-1.

Put $m=2^l$; then $m-1=2^l-1$ divides $m^k-1=2^{kl}-1$.

Finally, suppose (arguing by contradiction) that 2^n-1 is prime but n is composite, say $n=kl$ where k and l are greater than 1. Then 2^l-1 divides 2^n-1; and 2^l-1 is not 1 (since $l>1$ and is not 2^n-1 (since $l<n$). But this contradicts the assumption that 2^n-1 is prime.

1.25 Suppose that multiplication of polynomials satisfies the commutative law: that is, $f(x)g(x)=g(x)f(x)$ for any two polynomials $f(x)$ and $g(x)$.

Taking polynomials of degree zero, say $f(x)=a$, $g(x)=b$, we see that $ab=ba$; so multiplication of the coefficients is commutative.

Taking polynomials of degree 1, say $f(x)=ax+b$, $g(x)=x+1$, we see that

$$(ax+b)(x+1)=ax^2+(a+b)x+b=ax^2+(b+a)x+b.$$

We conclude that $a+b=b+a$, so that addition is commutative.

Finally, taking polynomials of degree 2, say $f(x)=ax^2+bx+c$ and $g(x)=x^2+x+1$, we see that the term in x^2 in $(ax^2+bx+c)(x^2+x+1)$ and $(x^2+x+1)(ax^2+bx+c)$ are $(a+b)+c$ and $(c+b)+a=a+(b+c)$, respectively; so the addition must be associative. (I assumed that in adding up three numbers we add the first two and then add the result to the third.)

If you were watching closely, you will see that I have used the number 1 as a coefficient of the polynomials in this argument. Is this essential?

1.27 On page 33, we saw that $A\subseteq B$ means

$$(x\in A)\Rightarrow(x\in B)$$

for all elements x. Also, $B \subseteq A$ means

$$(x \in B) \Rightarrow (x \in A)$$

for all x. So both conditions together are equivalent to

$$(x \in A) \Leftrightarrow (x \in B)$$

for all x; and this is the definition of $A = B$.

1.29 A function $f : \{1,2,\ldots,n\} \to A$ is specified by n values $f(1), f(2), \ldots, f(n)$. So for every function f, we can construct an element of A^n (an n-tuple $(a_1,\ldots,a_n)$ of elements of A), where $a_1 = f(1)$, $a_2 = f(2)$, ..., $a_n = f(n)$. This defines a function F from the set of functions to A^n. We see that

- F is one-to-one: since if $F(f) = F(g)$, then $f(i) = g(i)$ for all i, so $f = g$ as functions.
- F is onto: given any n-tuple $(a_1,\ldots,a_n)$, we can define a function f which maps 1 to a_1, ..., n to a_n. Formally, as a set of ordered pairs, we have

$$F = \{(1,a_1),(2,a_2),\ldots,(n,a_n)\}.$$

So F is a bijection between these two sets.

1.31 (a) If we put 0 into the black box, there is no output: $1/0$ is not defined. We could say instead

$$F(x) = \begin{cases} 1/x & \text{if } x \neq 0, \\ 0 & \text{if x=0.} \end{cases}$$

(b) This is a bit more subtle. The roots of the quadratic $x^2 - 3x + 2 = 0$ are $x = 1$ and $x = 2$: so is $F(-3,2) = (1,2)$ or is it $(2,1)$? We are given no rule to decide.

The problem can be resolved by inventing a rule about which of the two roots to put first. For example, if the real parts of the two roots are unequal, we could put the one with smaller real part first; if the real parts are equal but the imaginary parts are unequal, we could put the one with smaller imaginary part first; and if both real and imaginary parts are equal, then the two roots are equal, and it doesn't matter which one we put first! In the example, this rule would give $F(-3,2) = (1,2)$. Any rule would do as long as it gives a definite result.

A more sophisticated idea is to change the definition of the codomain of the function. Let $\mathbb{C}^{\{2\}}$ denote the set of all subsets of $\mathbb{C}$ consisting of one or two elements. Then the function F maps $\mathbb{C}^2 \to \mathbb{C}^{\{2\}}$. The point is that the two roots of the quadratic form a set with two elements (if they are unequal) or one element (if they are equal), and the order is not important.

1.33 An equivalence relation on A is a certain set of ordered pairs of elements of A. If A is the empty set, there can be no pairs, so the only relation on A is the "empty relation", and you can check that the empty relation is an equivalence relation. So there is one equivalence relation on the empty set.

The parts of a partition are required to be non-empty, so at first you might think that there are no partitions of the empty set. But it is not required that the *set of parts* is non-empty! So, again, there is one partition of the empty set, namely the empty set of subsets.

So the Equivalence Relation Theorem is valid.

1.35 It is easier to describe the five partitions:

$$\{\{1,2,3\}\}$$
$$\{\{1\},\{2,3\}\}$$
$$\{\{1,2\},\{3\}\}$$
$$\{\{1,3\},\{2\}\}$$
$$\{\{1\},\{2\},\{3\}\}$$

(As a subsidiary exercise, write out the equivalence relation corresponding to each partition. In the last case it is the relation of equality.)

There are fifteen equivalence relations on a set of size 4. Of these, one has a single part; four have parts of sizes 1 and 3; three have parts of sizes 2 and 2; six have parts of sizes 1, 1 and 2; and one has four parts of size 1.

Remark The number of partitions of a set of size n is called the n-th *Bell number* and is denoted by B_n. As a further exercise, show that $B_0 = 1$ and, for $n > 0$,

$$B_n = \sum_{k=1}^{n} \binom{n-1}{k-1} B_{n-k}.$$

You can use this relation to check that $B_3 = 5$ and $B_4 = 15$.

1.37 Let $[a]$ denote the equivalence class of $\mathrm{KER}(F)$ containing the element a. Thus, $[a]$ consists of all elements $a' \in A$ for which $F(a') = F(a)$.

Define ϕ from the set of equivalence classes of $\mathrm{KER}(F)$ to B by $\phi([a]) = F(a)$. This is well-defined because, if we had chosen a different representative a' of $[a]$, then $F(a) = F(a')$ by definition. The function ϕ actually maps onto $\mathrm{Im}(F)$. If is one-to-one; for, if $\phi([a_1]) = \phi([a_2])$, then $F(a_1) = F(a_2)$, so that a_1 and a_2 actually lie in the same equivalence class of $\mathrm{KER}(F)$: that is, $[a_1] = [a_2]$. So ϕ is a bijection.

1.39 (a) We show that $\equiv$ is an equivalence relation.

- Choose $x \in X$. Then $x \sim x$ and $x \sim x$ (because $\sim$ is reflexive); so $x \equiv x$ by definition. So $\equiv$ is reflexive.
- Suppose that $x \equiv y$. Then, by definition, $x \sim y$ and $y \sim x$; so $y \sim x$ and $x \sim y$, whence $y \equiv x$. Thus $\equiv$ is symmetric.
- Suppose that $x \equiv y$ and $y \equiv z$. Then $x \sim y$ and $y \sim z$, so $x \sim z$ (since $\sim$ is transitive). Also $z \sim y$ and $y \sim x$, so $z \sim x$. Thus $x \equiv z$; and so $\equiv$ is transitive.

(b) We are given that $x \sim y$, and that $x \equiv x_1$ and $y \equiv y_1$. Then $x_1 \sim x$; $x \sim y$; and $y \sim y_1$. By transitivity of $\sim$, we have $x_1 \sim y_1$ as required.

Remark This means that there is a relation $\leq$ defined on the set of equivalence classes of $\equiv$ by the rule

$$[x] \leq [y] \text{ if and only if } x \sim y.$$

(Part (b) shows that this relation is well-defined, independent of the choice of representatives.) Now, if $[x] \leq [y]$ and $[y] \leq [x]$, then $x \sim y$ and $y \sim x$, so $x \equiv y$ and $[x] = [y]$.

Thus the relation $\leq$ is irreflexive and transitive, and is a partial order on the equivalence classes.

A reflexive and transitive relation such as $\sim$ is called a **preorder**.

1.41 More empty set theory! If A is the empty set, then A^2 is also the empty set, and it has just one subset, namely itself. So there is only one candidate for a function from A to A. This "empty function" really is a function, and it is one-to-one and onto, so is a permutation. (Here is one way to see this. Could the empty function F fail to be one-to-one? This could only happen if there exist two different points $a_1, a_2 \in A$ such that $F(a_1) = F(a_2)$; but this can never happen since there are no points in A. Similarly, could it fail to be onto? This could only happen if there is a point in A to which nothing is mapped by F. But there is no point in A.)

1.43 The order of a permutation is the least common multiple of its cycle lengths. So, if the order is odd, then every cycle length is odd. Now to decide on the parity of a permutation, we calculate $n-c$, where c is the number of cycles. If the cycle lengths are $x_1, \ldots, x_c$, then

$$n - c = (x_1 - 1) + (x_2 - 1) + \cdots + (x_c - 1),$$

and if all the cycle lengths are odd, then each term $x_i - 1$ is even, and the sum is even.

The converse is false. The permutation $(1,2)(3,4)$ has order $\mathrm{lcm}(2,2) = 2$ which is even, but $n - c = 4 - 2 = 2$ so it is an even permutation.

1.45 (a) The binomial coefficient $\binom{p}{k}$ is given by the formula

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots 1}{k\cdots 1 \cdot (p-k)\cdots 1}.$$

There is a factor p in the numerator but no factor p in the denominator, since $1 \leq k \leq p-1$. As p is prime, it cannot be cancelled out by any of the factors in the denominator (which are all smaller than p). So the result is a multiple of p. (b) The proof is by induction on n. For $n = 1$, we certainly have $1^p = 1$, so $1^p \equiv_p 1$.

For the inductive step we assume that $n^p \equiv_p n$ and have to prove that $(n+1)^p \equiv_p n+1$. By the Binomial Theorem we have

$$(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k 1^{p-k} = n^p + \sum_{k=1}^{p-1} \binom{p}{k} n^k + 1.$$

By part (a), all the terms in the sum from $k = 1$ to $p-1$ are multiples of p, and so all this part of the expression is divisible by p. Thus we have

$$(n+1)^p \equiv_p n^p + 1 \equiv_p n + 1,$$

where the second step comes from the induction assumption $n^p \equiv_p n$.

By induction, the statement $n^p \equiv_p n$ is proved for all $n \geq 1$.

1.47 Let

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, C = \begin{pmatrix} p & q \\ r & s \end{pmatrix}.$$

The distributive law asserts that $A(B+C) = AB+AC$. I will do only part of the calculation here; you can complete it yourself.

We have

$$A(B+C) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e+p & f+q \\ g+r & h+s \end{pmatrix} = \begin{pmatrix} a(e+p)+b(g+r) & \dots \\ \dots & \dots \end{pmatrix},$$

while

$$AB+AC = \begin{pmatrix} ae+bg & \dots \\ \dots & \dots \end{pmatrix} + \begin{pmatrix} ap+br & \dots \\ \dots & \dots \end{pmatrix}.$$

So we have to show that

$$a(e+p)+b(g+r) = (ae+bg)+(ap+br).$$

To do this, we expand the brackets on the left (using the distributive law) to get $(ae+ap)+(bg+br)$. Then re-position the brackets (using the associative law for addition) to get $ae+(ap+bg)+br$. Then interchange the two terms in brackets (using the commutative law for addition) to get $ae+(bg+ap)+br$, and finally rearrange the brackets again to get $(ae+bg)+(ap+br)$.

So we use the distributive law and the associative and commutative laws for addition in the proof.

1.49 Let $A = (a_{ij})$ and $B = (b_{ij})$ be upper triangular matrices. This means that, if $i > j$, then $a_{ij} = b_{ij} = 0$. Let $A+B = C = (c_{ij})$, so that $c_{ij} = a_{ij} + b_{ij}$. If $i > j$, then $c_{ij} = a_{ij} + b_{ij} = 0+0 = 0$, so C is upper triangular.

Now let $AB = D = (d_{ij})$, so that $d_{ij} = \sum_{k=0}^{n} a_{ik}b_{kj}$. Now suppose that $i > j$. For each value of k, either $i > k$ or $k > j$. (For if this were not so, then $i \leq k$ and $k \leq j$, which would imply $i \leq j$, contrary to our assumption.) This means that either a_{ik} or b_{kj} is zero, so that their product is zero. But then every term in the sum is zero, so that $d_{ij} = 0$. This shows that D is upper triangular.

The multiplication is not commutative. Here is an example:

$$\begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 4 \\ 0 & 2 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 2 \end{pmatrix}.$$

1.51 Subtracting twice the first equation from the second, and three times the first from the third, gives

$$\begin{aligned} y+4z &= 6, \\ 2y+8z &= c-30. \end{aligned}$$

Now subtracting twice the first (new) equation from the second gives $0 = c-42$. So there is no solution unless $c = 42$.

If $c = 42$, then we have shown that the last equation is a consequence of the other two, so can be deleted. Now we can take z to be arbitrary, and find $y = 6-4z$, $x = 10-2y-3z = 5z-2$.

1.53 The truth table looks like this:

p	q	$p \Rightarrow q$	$q \Rightarrow p$	$(p \Rightarrow q) \vee (q \Rightarrow p)$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	T
F	F	T	T	T

Since the formula always has the value T, it is logically valid.

The result could be stated informally: "Given any two propositions, one logically implies the other", which sounds paradoxical!

1.55 $x \in A \triangle B$ holds if (and only if) $x \in A$ or $x \in B$, but not both. So we have to show that $\neg(p \Leftrightarrow q)$ is true if and only if one of p and q is true and the other false. This is the same as showing that $p \Leftrightarrow q$ is true if and only if both or neither of p and q is true, which is precisely the definition of $\Leftrightarrow$.

The formula $p \Rightarrow q$ is true in all cases except where p is true and q is false, that is, in all cases except where $x \in A$ and $x \notin B$. In other words, the corresponding set is the complement of $A \cap B'$, which (by De Morgan's Law) is $A' \cup B$.